Newsroom

December 13, 2010

Georgia Southern University

Georgia Southern University Faculty Expert Offers Online Shopping Security Tips

DECEMBER 13, 2010

Thanks to the World Wide Web and e-promotions on everything from gadgets to groceries, each year more people choose to tackle their holiday shopping list from the comfort of their own home. Many conservative consumers often wonder about safety issues associated with buying online, but Georgia Southern University professors say that — excluding situations with obvious red flags —online stores are usually just as safe as the ones filled with bargain-hungry shoppers.

Information Systems department chair Tom Case said some consumers are wary because of the lack of interpersonal contact and misconceptions about the online buying process.

"Many of these people will refuse to enter their personal information into a secure shopping site, but have no problem handing over their credit card to a server, who takes it out of their site for several minutes. In my book, the latter situation brings about a much greater cause for concern," said Case, who has taught at Georgia Southern for 29 years. "There are true red flags to watch out for, but with payments primarily processed electronically in stores as well, the risk for fraud isn't greatly increased online."

Case added that major retailers and brands have a lot to lose by not protecting the personal and financial information of their customers. They have taken extreme measures to ensure this data is protected. For instance, online "wallets" that save billing information may seem risky to some, but are actually very safe. Bank account and credit card numbers are saved in secure databases and their display is encrypted — which is actually safer than entering this information with each purchase.

Although security measures have improved substantially in recent years, Case warns that consumers should remain diligent regardless of their medium for purchase.

"Identity theft is not an unfounded fear, but to abstain from making purchases online is extreme," Case said. "Be cautious in all purchases. Never relinquish your credit card for long periods of time and beware of the risks when you let anyone take it out of sight. Remember also that there are very few situations — and absolutely no shopping/purchasing situations —where providing your social security number is necessary."

Guide to safe online shopping:

1) When "checking out," watch for the address bar displaying the Web address to change from "http" to "https." The S indicates you are entering a secure site.

2) Look for the secure site lock icon in your browser's status bar.

3) On sites for which you have never purchased, look for clickable icons like:

Today, these are rarely found on major retailer and online merchant sites, but are often displayed on lesser known or regional merchants to communicate to their web site visitors that the safety of their online purchasing and payment systems have been verified by trusted third- party evaluators. When BBB or VeriSign icons are clicked, visitors are directed to pages at the BBB or VeriSign confirming that the site is legitimate (check the URL for the verification page to ensure you are actually viewing BBB or VeriSign report pages.

4) Never give your social security number. Don't be as concerned about providing an email address or phone number — there is little they could gain from this information.

5) Make sure your credit card policy offers adequate fraud protection. Some even monitor your purchase habits and lock down use after abnormal spending occurs. Others require users to repay only a small amount, or none of fraudulent online charges.

6) Consider having more than one e-mail address and use a generic account (gmail, hotmail or yahoo) for purchases and promotional mailings. Do not use a work address.

7) If you do encounter online scams, report it.

8) Case suggests consumers watch for these red flags:

1. Shopping sites that require your social security number.
2. Sites that require you to make a phone call to a personal number for purchase. Many are legitimate businesses that haven't yet mastered their Web skills, but others are scams, so proceed with caution.
3. Beware of any electronic transaction that requires you to wire money to complete the purchase.
4. E-mails that route you to sites asking for verification of personal information or passwords — even if they look exactly like the business's real site — are often phishing scams. Also, be careful of situations where you are unnecessarily redirected to a website.
5. Remember, purchases should be initiated by the consumer. Be wary of emails and links that take you directly to a purchasing/checkout page.
6. Exercise caution with online purchasing sites that have social networking URL's (Facebook, MySpace, etc.). Scammers and fraudsters are working hard to exploit the security vulnerabilities.

< Previous Next >